STATE OF ALASKA

DEPARTMENT OF LAW

OFFICE OF THE ATTORNEY GENERAL

FRANK H. MURKOWSKI, GOVERNOR

1031 WEST 4TH AVENUE, SUITE 200
ANCHORAGE, ALASKA 99501-5903
PHONE: (907)269-5100
FAX: (907)276-8554

February 4, 2005

Dear Consumer,

National Consumer Protection Week is February 6-12, 2005. The subject of this year's NCPW is **Identity Theft: When Fact Becomes Fiction**.

Identify theft is one of the fastest-growing crimes in the nation. Identity thieves can capture information about you and use it to commit fraud, steal your money, charge items on your credit cards, and even apply for jobs in your name. It's a crime that can wreak havoc on your finances, your credit, and your reputation.

The good news is that there are steps that you can take to minimize your risk of becoming a victim of identity theft. The enclosed materials provide information on how you can safeguard your personal information and what to do if you become a victim. Also, the Consumer Protection Unit's web site at www.law.state.ak.us/consumer/ has information on identity theft and other consumer matters. You can download a consumer complaint form and file it with this office if you believe that you've been the victim of an unfair trade practice.

Thank you for your interest in preventing identity theft and in National Consumer Protection Week.

Sincerely,

GREGG D. RENKES
ATTORNEY GENERAL

State of Alaska

Department of Law

Gregg Renkes
Attorney General
P.O. Box 110300
Juneau, Alaska 99811-0300

NEWS RELEASE

Mark Morones
Press Contact
907-269-6393
FAX: 907-269-6305
www.law.state.ak.us

FOR IMMEDIATE RELEASE: February 4, 2005

National Consumer Protection Week Focuses on Identity Theft:

Attorney General and AARP Chapters Launch Tandem Efforts to Educate and Protect Alaskans

(Juneau) – Attorney General Gregg Renkes has joined a group of federal, state and local agencies and national advocacy groups, including the AARP, to launch the seventh annual National Consumer Protection Week (NPCW), February 6-12, 2005, highlighting consumer protection and education efforts around the country.

This year's NPCW theme, "Identity Theft: When Fact Becomes Fiction," focuses on minimizing the risk and containing the harm of identity theft. "I encourage all Alaskans to know how to protect their personal information," said Renkes. "Safeguarding your personal information, reviewing your credit reports and using strong passwords on personal computers are a few important steps consumers can take to minimize the risk of identity theft."

Consumers may call the Attorney General's Office at (907) 269-5100 to request a copy of the "identity theft" packet created specifically for NCPW. Brochures from this packet may also be downloaded from the Attorney General's consumer protection website at: www.law.state.ak.us/consumer. The Federal Trade Commission (FTC) also offers a significant amount of information on this topic available online at: www.consumer.gov/ncpw.

"The past several years has seen significant growth in our state's senior population and an overall increase in the use of the Internet as a home personal and financial planning tool," said Renkes. It is unavoidable that older Alaskans will be increasingly exploited by scams. Education is a critical component of our future plans to target these types of illegal activities."

In the next few days and weeks, representatives from the Department of Law will be making the case for increasing its budget to address fraud against Alaska's seniors, including identity theft. Similar efforts have already taken place in many other states.

More

(ID Theft press release, con't.)

"Seniors are especially vulnerable to the increasingly diverse rip-off schemes that are on the rise across the country. According to the FTC, identity theft among seniors alone increased 218 percent between 2001 and 2002," said Renkes. "That is why this legislative session we are asking the legislature to fund the creation of a special unit dedicated to fraud targeted at Alaska's seniors. The two-fold goal of this program is to educate potential victims and prosecute those who would attempt to prey on Alaska's senior population."

If this proposal is funded, two new attorney positions and an investigator position will be created to focus on this effort.

In addition to efforts within the Department of Law related to the growing problem of identity theft, a number of organizations are focusing on education efforts targeted for seniors.

Representatives from the AARP's national consumer protection league will conduct seminars in four Alaska cities next week, to educate members of the public on identity theft and a number of other topics ranging from investment scams to payday lending. The events are open to the public at the following dates and locations:

- **Tuesday, February 7th in Anchorage**, from 9:00 a.m. to 1:00 p.m., at the Anchorage Senior Center, 1300 E. 19th Avenue. Contact: Chuck Lyons, AARP Sourdough Chapter President at 243-4601
- **Wednesday, Feb. 8th in Ketchikan**, from 10:00 a.m. to 2:00 p.m., at the Pioneer Hall, #2 Pioneer Alley. Contact: Ed Zastrow at 907-225-2814.
- **Thursday, Feb. 9th in Juneau**, from 9:00 a.m. to 1:00 p.m., at Fireweed Place, 415 Willoughby Ave. Contact: Liz Lucas, AARP Alaska State President at (907) 789-9655.
- **Friday, Feb 11th in Fairbanks**, from 9:00 a.m. to 1:00 p.m., at the Noel Wien Library, 1215 Cowles. Contact: Karen Wood, Secretary, AARP Chapter #770, 907-452-2277

Governor Frank H. Murkowski will bring attention to the rising threat of identify theft in Alaska in a proclamation to be released, via the web, on Monday, Feb. 7. A copy of the proclamation can be found at: http://gov.state.ak.us/proclamations.php.

For additional information, please contact Mark Morones, Special Assistant for Communications for the Department of Law at (907) 269-6393. For additional information regarding the AARP seminars, please contact Ann Secrest at (907) 762-3302 or toll free at (866) 227-7447.

# # #

IDENTITY THEFT FACT SHEET

Source: FTC's NCPW 2005. Quiz – Identity Theft: When Fact Becomes Fiction

1. ID theft is the fastest growing white-collar crime in the U.S. 27 million Americans have been victims of the crime in the past five years, nearly 10 million people last year.
2. Identity thieves can get personal information from you by:
   - Stealing your wallet or purse
   - Stealing your mail
   - Rummaging through your trash, and
   - Using personal information they find on the Internet about you.

For additional information on how ID thieves can steal your identity, go to: www.consumer.gov/idtheft/understanding_idt.html#2.

3. If you are getting rid of your computer, it is not enough to delete files using mouse and keyboard commands. Use a "wipe" utility program to overwrite the entire hard drive. This makes files unrecoverable.
4. ID thieves that obtain your personal information can: (1) call your credit card issuer and change the mailing address on your card; (b) open a new credit card account or bank account in your name; (c) file for bankruptcy under your name to avoid paying off debts they've incurred; and (d) counterfeit checks or drain your bank account.
5. Here are some ways for you to minimize your risk of becoming a victim of ID theft::
   - Don't give out personal information by email, Internet, phone or mail unless you initiated contact and you are certain you know who you are dealing with
   - Don't carry your social security card with you
   - Carry only the identification information and credit/debit cards that you actually need
   - Password protect your credit card, bank and phone accounts.
   - For additional tips, go to: www.consumer.gov/idtheft/protect_againstidt.html#5.
6. If you are a victim of ID theft, place a fraud alert on your credit report. This will help prevent If thieves from opening additional accounts in your name.
7. If you think someone has stolen your personal information or identification, do the following:
   - Immediately close all your credit card or bank accounts
   - Place a fraud alert with any one of the three national consumer reporting companies
   - Contact the Social Security Administration to get a new Social Security number
   - Alert issuing agencies for your driver's license and other identification documents
8. If you have high speed Internet connection, such as DSL or cable modem, get a firewall program to prevent uninvited guests from accessing your computer.
9. Signs you could be a victim of ID theft:
   - Fail to receive bills or other mail
   - Receive credit cards for which you did not apply
   - Are denied credit for no apparent reason
   - Get calls or letters from debt collectors or businesses about merchandise or services you didn't buy
10. Don't tape computer and website passwords to your computer. Safeguard these passwords. Also, when creating passwords, use a combination of letters (upper and lower case), numbers and symbols.

IDENTITY THEFT IN ALASKA

Source: FTC's Consumer Sentinel Complaint Statistics and Trends for Alaska, for the periods January 1 – December 31, 2004, (pg. 17 of 66) & January 1 – December 31, 2003 (pg. 17 of 66)
http://www.consumer.gov/sentinel/pubs/Top10Fraud2004.pdf

Fraud complaints from Alaska consumers:

- 1,143 in 2004
- 1,165 in 2003

Identity theft complaints from Alaska victims:

- 433 in 2004
- 231 in 2003

Ranking ID theft by category from Alaska victims in 2004 – Identity Theft Complaints from Alaska Victims = 433

Rank	Type	# of Victims	Percentage*
1	Credit card fraud	127	29%
2	Phone or utilities fraud	78	18%
3	Bank fraud**	59	14%
4	Gov't documents or benefits fraud	33	8%
5	Employment-related fraud	30	7%
6	Loan fraud	18	4%
	Other	129	30%
	Attempted ID theft	31	7%

* Percentages are based on 433 victims reporting from Alaska. Percentages add to more than 100 because approximately 17% of victims from Alaska reported experiencing more than one type of identity theft.

** Includes fraud involving checking and savings accounts and electronic fund transfers.

Ranking ID theft by category from Alaska victims in 2003 – Identity Theft Complaints from Alaska Victims = 231

Rank	Type	# of Victims	Percentage*
1	Credit card fraud	80	35%
2	Phone or utilities fraud	35	15%
3	Bank fraud**	32	14%
4	Employment-related fraud	23	10%
5	Gov't documents or benefits fraud	17	7%
6	Loan fraud	15	6%
	Other	64	28%
	Attempted ID theft	18	8%

* Percentages are based on 231 victims reporting from Alaska. Percentages add to more than 100 because approximately 17% of victims from Alaska reported experiencing more than one type of identity theft.

** Includes fraud involving checking and savings accounts and electronic fund transfers.

FRANK H. MURKOWSKI,
GOVERNOR

DEPARTMENT OF LAW

OFFICE OF THE ATTORNEY GENERAL

1031 WEST 4TH AVENUE, SUITE 200
ANCHORAGE, ALASKA 99501-5903
PHONE: (907)269-5100
FAX: (907)276-8554

TOP 10 TIPS FOR IDENTITY THEFT PREVENTION
Consumer Protection Unit
February 2005

1. **Check your credit reports – for free.** Federal law allows you to receive a free copy of your credit report each year. Obtain a copy from each of the three major credit reporting agencies every year. Make sure it is accurate, current and includes only those activities you have authorized or are aware of.

2. **Protect your Social Security number.** Give your Social Security Number only when it is absolutely necessary. Ask to use other types of identifiers when possible. Don't carry your Social Security card in your wallet.

3. **Keep your computer safe.** Protect your personal information on your home computer. Use strong passwords that contain at least eight characters and include a combination of letters, numbers, and symbols. Passwords should be easy for you to remember, but difficult for others to guess. Use firewall and virus protection software that you update regularly. Steer clear of spyware; download free software only from sites you know and trust. Don't install software without knowing what it is. Set Internet Explorer browser security to at least "medium." Don't click on links in pop-up windows or on spam e-mail.

4. **Carefully review your bills and bank statements.** Open and review your credit card bills and bank statements right away. If you notice odd charges, contact your creditors or bank immediately.

5. **Pay attention to your billing cycles.** If your bills do not arrive on time, follow up with creditors. A missing credit card bill could mean an identity thief has taken

over your credit card account and changed your billing address to cover his or her tracks.

6. **Shred or tear papers with personal information.** To protect your personal information from thieves who steal from trash or recycling bins, tear or shred your charge receipts, copies of credit applications, insurance forms, physician statements, telephone and other utility bills, bank checks and statements you are discarding, expired charge cards and credit offers that you get in the mail.

7. **Use caution online.** When shopping online, check out a web site before entering your credit card number or other personal information. Only enter personal information on secure web pages with "https" in the address bar and a padlock symbol at the bottom of the browser window. These are signs that your information will be encrypted or scrambled, protecting it from hackers.

8. **Stop pre-approved credit offers.** Stop most pre-approved credit card offers. They make a tempting target for identity thieves who steal your mail. Have your name removed from credit bureau marketing lists. Call toll-free 888-5OPTOUT (888-567-8688).

9. **Don't get hooked by a "phishing" scam.** Phishing is a high-tech scam that uses spam or pop-up messages to deceive you into disclosing your personal information. Phishers will send you an e-mail or pop-up message that claims to be from a business or organization that you deal with – for example, your bank, internet service provider, or even a government agency. They usually say that you need to "update" or "validate" your account information and they often threaten some dire consequence if you don't respond. You should not reply or click on the link in the message. Legitimate companies don't ask for information this way. If you are concerned about your account, contact the organization using a telephone number you know to be genuine.

10. **Ask questions.** Ask questions whenever you are asked for personal information that seems inappropriate for the transaction. Ask how the information will be used and if it will be shared. Ask how it will be protected. Explain that you're concerned about identity theft. If you're not satisfied with the answers, consider doing business somewhere else.

December 17, 2004

Free Credit Reports for Alaskans

The Consumer Protection Unit recommends that you take advantage of a recent change in the federal Fair Credit Reporting Act (FCRA) that allows you to obtain free copies of your credit reports each year. Alaskans and residents of other western states have been eligible to order their free reports since December 1, 2004; residents of other states will be able to obtain their free reports at later dates.

Credit reports contain information on where you live, how you pay your bills, and whether you've been sued, arrested, or filed for bankruptcy. There are three nationwide companies that compile this information and sell it to creditors, insurers, employers, and others. These companies are Experian, Equifax, and Trans Union. You can obtain a free report from each company once every 12 months.

By regularly reviewing your credit report, you can check to make sure the information in it is correct and complete. Having an accurate report is important when you apply for a loan for a house or car, buy insurance, or apply for certain jobs. And reviewing your credit report will also help guard against identity theft. Identity theft happens when an identity thief uses your personal information – such as your name, Social Security Number, or credit card number – to open a new credit card account or obtain a loan or take other action pretending to be you. When the thief becomes delinquent on an account or fails to make a loan payment, it gets reported on your credit report. To learn more about identity theft and what to do if you've been a victim, go to http://www.consumer.gov/idtheft/.

For more information about obtaining your free credit report and your rights under the FCRA, go to http://www.ftc.gov/bcp/conline/pubs/credit/freereports.htm.

CREDIT

FEDERAL TRADE COMMISSION 1-877-FTC-HELP WWW.FTC.GOV FOR THE CONSUMER

FTC FACTS for Consumers

YOUR ACCESS TO FREE CREDIT REPORTS

Soon you'll be able to get your credit report for free. A recent amendment to the federal Fair Credit Reporting Act (FCRA) requires each of the nationwide consumer reporting companies to provide you with a free copy of your credit report, at your request, once every 12 months. The FCRA promotes the accuracy and privacy of information in the files of the nation's consumer reporting companies. The Federal Trade Commission (FTC), the nation's consumer protection agency, enforces the FCRA with respect to consumer reporting companies.

A credit report contains information on where you live, how you pay your bills, and whether you've been sued, arrested, or filed for bankruptcy. Nationwide consumer reporting companies sell the information in your report to creditors, insurers, employers, and other businesses that use it to evaluate your applications for credit, insurance, employment, or renting a home. There are three nationwide consumer reporting companies — Equifax, Experian, and Trans Union.

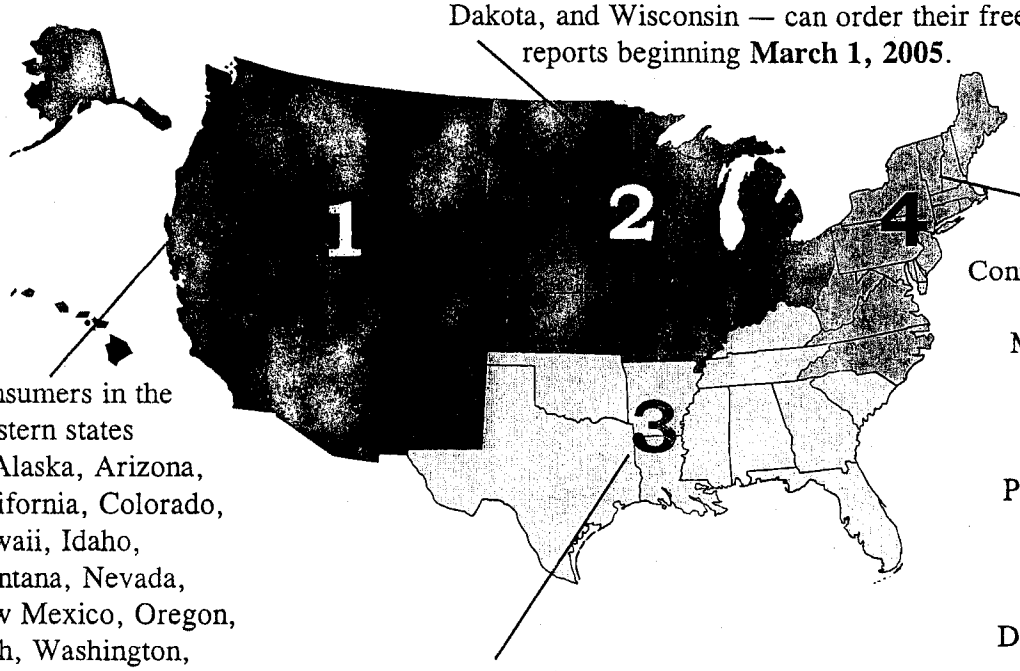
Consumers in Western states will first be able to order their credit reports under the federal law beginning December 1, 2004. Consumers in other states will be able to order their copies according to a regional roll-out detailed below.

In recent months, consumers have asked the FTC for more details about their rights under the federal FCRA and the Fair and Accurate Credit Transactions (FACT) Act, which established the free credit report program. They've also asked about credit reports in general. Here are the most frequently asked questions and the answers.

Q: How do I know when I'm eligible to get a free report?

A: Free reports will be phased in during a nine-month period, rolling from the West Coast to the East beginning December 1, 2004. Beginning September 1, 2005, free reports will be accessible to all Americans, regardless of where they live.

MAP OF FREE CREDIT REPORT ROLL-OUT



Consumers in the Midwestern states — Illinois, Indiana, Iowa, Kansas, Michigan, Minnesota, Missouri, Nebraska, North Dakota, Ohio, South Dakota, and Wisconsin — can order their free reports beginning **March 1, 2005**.

Consumers in the Western states — Alaska, Arizona, California, Colorado, Hawaii, Idaho, Montana, Nevada, New Mexico, Oregon, Utah, Washington, and Wyoming — can order their free reports beginning **December 1, 2004**.

Consumers in the Southern states — Alabama, Arkansas, Florida, Georgia, Kentucky, Louisiana, Mississippi, Oklahoma, South Carolina, Tennessee, and Texas — can order their free reports beginning **June 1, 2005**.

Consumers in the Eastern states — Connecticut, Delaware, Maine, Maryland, Massachusetts, New Hampshire, New Jersey, New York, North Carolina, Pennsylvania, Rhode Island, Vermont, Virginia, and West Virginia — the District of Columbia, Puerto Rico, and all U.S. territories can order their free reports beginning **September 1, 2005**.

Q: How do I order my free report?

A: The three nationwide consumer reporting companies have set up one central website, toll-free telephone number, and mailing address through which you can order your free annual report. To order, click on www.annualcreditreport.com, call 877-322-8228, or complete the Annual Credit Report Request Form and mail it to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. The form is on the back of this brochure; or you can print it from www.ftc.gov/credit. Do not contact the three nationwide consumer reporting companies individually. They are only providing free annual credit reports through www.annualcreditreport.com, 877-322-8228, and Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

You may order your reports from each of the three nationwide consumer reporting companies at the same time, or you can order from only one or two. The law allows you to order one free copy from each of the nationwide consumer reporting companies every 12 months.

Q: What information do I have to provide to get my free report?

A: You need to provide your name, address, Social Security number, and date of birth. If you have moved in the last two years, you may have to provide your previous address. To maintain the security of your file, each nationwide consumer reporting company may ask you for some information that only you would know, like the amount of your monthly mortgage payment. Each company may ask you for different information because the information each has in your file may come from different sources.

www.annualcreditreport.com is the only authorized source for your free annual credit report from the three nationwide consumer reporting companies. www.annualcreditreport.com and the nationwide consumer reporting companies will not send you an email asking for your personal information. If you get an email or see a pop-up ad claiming it's from www.annualcreditreport.com or any of the three nationwide consumer reporting companies, do not reply or click on any link in the message — it's probably a scam. Forward any email that claims to be from www.annualcreditreport.com or any of three consumer reporting companies to the FTC's database of deceptive spam at spam@uce.gov. www.annualcreditreport.com or any of three consumer reporting companies also will not call you to ask for your personal information.

Q: Why would I want to get a copy of my credit report?

A: You may want to review your credit report:

- because the information it contains affects whether you can get a loan — and how much you will have to pay to borrow money.
- to make sure the information is accurate, complete, and up-to-date before you apply for a loan for a major purchase like a house or car, buy insurance, or apply for a job.
- to help guard against identity theft. That's when someone uses your personal information — like your name, your Social Security number, or your credit card number — to commit fraud. Identity thieves may use your information to open a new credit card account in your name. Then, when they don't pay the bills, the delinquent account is reported on your credit report. Inaccurate information like that could affect your ability to get credit, insurance, or even a job.

Q: How long does it take to get my report after I order it?

A: If you request your report online at www.annualcreditreport.com, you should be able to access it immediately. If you order your report by calling toll-free 877-322-8228, your report will be processed and mailed to you within 15 days. If you order your report by mail using the Annual Credit Report Request Form, your request will be processed and mailed to you within 15 days of receipt.

Whether you order your report online, by phone, or by mail, it may take longer to receive your report if the nationwide consumer reporting company needs more information to verify your identity.

There may be times when the nationwide consumer reporting companies receive an extraordinary volume of requests for credit reports. If that happens, you may be asked to re-submit your request. Or, you may be told that your report will be mailed to you sometime after 15 days from your request. If either of these events occurs, the nationwide consumer reporting companies will let you know.

Q: Are there any other situations where I might be eligible for a free report?

A: Under federal law, you're entitled to a free report if a company takes adverse action against you, such as denying your application for credit, insurance, or employment, and you ask for your report within 60 days of receiving notice of the action. The notice will give you the name, address, and phone number of the consumer reporting company. You're also entitled to one free report a year if you're unemployed and plan to look for a job within 60 days; if you're on welfare; or if your report is inaccurate because of fraud, including identity theft. Otherwise, a consumer reporting company may charge you up to $9 for another copy of your report within a 12-month period.

To buy a copy of your report, contact:

- Equifax
  800-685-1111
  www.equifax.com
- Experian
  888-EXPERIAN (888-397-3742)
  www.experian.com
- Trans Union
  800-916-8800
  www.transunion.com

Under state law, consumers in Colorado, Georgia, Maine, Maryland, Massachusetts, New Jersey, and Vermont already have free access to their credit reports.

Q: Should I order a report from each of the three nationwide consumer reporting companies?

A: It's up to you. Because nationwide consumer reporting companies get their information from different sources, the information in your report from one company may not reflect all, or the same, information in your reports from the other two companies. That's not to say that the information in any of your reports is necessarily inaccurate; it just may be different.

Q: Should I order my reports from all three of the nationwide consumer reporting companies at the same time?

A: You may order one, two, or all three reports at the same time, or you may stagger your requests. It's your choice. Some financial

advisors say staggering your requests during a 12-month period may be a good way to keep an eye on the accuracy and completeness of the information in your reports.

Q: What if I find errors — either inaccuracies or incomplete information — in my credit report?

A: Under the Fair Credit Reporting Act, both the consumer reporting company and the information provider (that is, the person, company, or organization that provides information about you to a consumer reporting company) are responsible for correcting inaccurate or incomplete information in your report. To take advantage of all your rights under this law, contact the consumer reporting company and the information provider.

1. Tell the consumer reporting company, in writing, what information you think is inaccurate.

   Consumer reporting companies must investigate the items in question — usually within 30 days — unless they consider your dispute frivolous. They also must forward all the relevant data you provide about the inaccuracy to the organization that provided the information. After the information provider receives notice of a dispute from the consumer reporting company, it must investigate, review the relevant information, and report the results back to the consumer reporting company. If the information provider finds the disputed information is inaccurate, it must notify all three nationwide consumer reporting companies so they can correct the information in your file.

   When the investigation is complete, the consumer reporting company must give you the written results and a free copy of your report if the dispute results in a change. (This free report does not count as your annual free report under the FACT Act.) If an item is changed or deleted, the consumer reporting company cannot put the disputed information back in your file unless the information provider verifies that it is accurate and complete. The consumer reporting company also must send you written notice that includes the name, address, and phone number of the information provider.

2. Tell the creditor or other information provider in writing that you dispute an item. Many providers specify an address for disputes. If the provider reports the item to a consumer reporting company, it must include a notice of your dispute. And if you are correct — that is, if the information is found to be inaccurate — the information provider may not report it again.

Q: What can I do if the consumer reporting company or information provider won't correct the information I dispute?

A: If an investigation doesn't resolve your dispute with the consumer reporting company, you can ask that a statement of the dispute be included in your file and in future reports. You also can ask the consumer reporting company to provide your statement to anyone who received a copy of your report in the recent past. You can expect to pay a fee for this service.

If you tell the information provider that you dispute an item, a notice of your dispute must be included any time the information provider reports the item to a consumer reporting company.

Q: How long can a consumer reporting company report negative information?

A: A consumer reporting company can report most accurate negative information for seven years and bankruptcy information for 10 years. There is no time limit on reporting information about criminal convictions; information reported in response to your application for a job that pays more than $75,000 a year; and information reported because you've applied for more than $150,000 worth of credit or life insurance. Information about a lawsuit or an unpaid judgment against you can be reported for seven years or until the statute of limitations runs out, whichever is longer.

Q: Who else can get a copy of my credit report?

A: The Fair Credit Reporting Act specifies who can access your credit report. Creditors, insurers, employers, and other businesses that use the information in your report to evaluate your applications for credit, insurance, employment, or renting a home are among those that have a legal right to access your report.

Q: Can my employer get my credit report?

A: Your employer can get a copy of your credit report only if you agree. A consumer reporting company may not provide information about you to your employer, or to a prospective employer, without your written consent.

For More Information

The FTC works for the consumer to prevent fraudulent, deceptive and unfair business practices in the marketplace and to provide information to help consumers spot, stop and avoid them. To learn more about credit issues and protecting your personal information, visit www.ftc.gov/credit.

To file a complaint or to get free information on other consumer issues, visit www.ftc.gov or call toll-free, 1-877-FTC-HELP (1-877-382-4357); TTY: 1-866-653-4261. The FTC enters Internet, telemarketing, identity theft and other fraud-related complaints into Consumer Sentinel, a secure, online database available to hundreds of civil and criminal law enforcement agencies in the U.S. and abroad.

Federal Trade Commission	www.ftc.gov
1-877-FTC-HELP	For The Consumer

November 2004

EQUIFAX experian TransUnion

Annual Credit Report Request Form

You have the right to get a free copy of your credit file disclosure, commonly called a credit report, once every 12 months, from each of the nationwide consumer credit reporting companies - Equifax, Experian and TransUnion.

For instant access to your free credit report, visit www.annualcreditreport.com.

For more information on obtaining your free credit report, visit www.annualcreditreport.com or call 877-322-8228.

Use this form if you prefer to write to request your credit report from any, or all, of the nationwide consumer credit reporting companies. The following information is required to process your request. **Omission of any information may delay your request.**

Once complete, fold (do not staple or tape), place into a #10 envelope, affix required postage and mail to:
Annual Credit Report Request Service P.O. Box 105281 Atlanta, GA 30348-5281.

Please use a Black or Blue Pen and write your responses in PRINTED CAPITAL LETTERS without touching the sides of the boxes like the examples listed below:

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z 0 1 2 3 4 5 6 7 8 9

Social Security Number: ___ - ___ - ____

Date of Birth: ___ / ___ / ____
Month / Day / Year

Fold Here ---------- Fold Here

First Name | **M.I.**

Last Name | **JR, SR, III, etc.**

Current Mailing Address:

House Number | **Street Name**

Apartment Number / Private Mailbox | **For Puerto Rico Only: Print Urbanization Name**

City | **State** | **ZipCode**

Previous Mailing Address (complete only if at current mailing address for less than two years):

House Number | **Street Name**

Fold Here ---------- Fold Here

Apartment Number / Private Mailbox | **For Puerto Rico Only: Print Urbanization Name**

City | **State** | **ZipCode**

Shade Circle Like This → ●

Not Like This → ⊗ ✓

I want a credit report from (shade each that you would like to receive):

- ○ **Equifax**
- ○ **Experian**
- ○ **TransUnion**

○ **Shade here if, for security reasons, you want your credit report to include no more than the last four digits of your Social Security Number.**

If additional information is needed to process your request, the consumer credit reporting company will contact you by mail.

Your request will be processed within 15 days of receipt and then mailed to you.

31238

FTC Consumer Alert

Federal Trade Commission ■ Bureau of Consumer Protection ■ Office of Consumer & Business Education

How Not to Get Hooked by a 'Phishing' Scam

Internet scammers casting about for people's financial information have a new way to lure unsuspecting victims: They go "phishing."

Phishing is a high-tech scam that uses spam or pop-up messages to deceive you into disclosing your credit card numbers, bank account information, Social Security number, passwords, or other sensitive information.

According to the Federal Trade Commission (FTC), phishers send an email or pop-up message that claims to be from a business or organization that you deal with – for example, your Internet service provider (ISP), bank, online payment service, or even a government agency. The message usually says that you need to "update" or "validate" your account information. It might threaten some dire consequence if you don't respond. The message directs you to a Web site that looks just like a legitimate organization's site, but it isn't. The purpose of the bogus site? To trick you into divulging your personal information so the operators can steal your identity and run up bills or commit crimes in your name.

The FTC, the nation's consumer protection agency, suggests these tips to help you avoid getting hooked by a phishing scam:

- If you get an email or pop-up message that asks for personal or financial information, **do not reply or click on the link in the message**. Legitimate companies don't ask for this information via email. If you are concerned about your account, contact the organization in the email using a telephone number you know to be genuine, or open a new Internet browser session and type in the company's correct Web address. In any case, don't cut and paste the link in the message.
- **Don't email personal or financial information.** Email is not a secure method of transmitting personal information. If you initiate a transaction and want to provide your personal or financial information through an organization's Web site, look for indicators that the site is secure, like a lock icon on the browser's status bar or a URL for a website that begins "https:" (the "s" stands for "secure"). Unfortunately, no indicator is foolproof; some phishers have forged security icons.
- **Review credit card and bank account statements** as soon as you receive them to determine whether there are any unauthorized charges. If your statement is late by more than a couple of days, call your credit card company or bank to confirm your billing address and account balances.
- **Use anti-virus software and keep it up to date**. Some phishing emails contain software that can harm your computer or track your activities on the Internet without your knowledge. Anti-virus software and a firewall can protect you from inadvertently accepting such unwanted files. Anti-virus software scans incoming communications for troublesome files. Look for anti-virus

software that recognizes current viruses as well as older ones; that can effectively reverse the damage; and that updates automatically.

A firewall helps make you invisible on the Internet and blocks all communications from unauthorized sources. It's especially important to run a firewall if you have a broadband connection. Finally, your operating system (like Windows or Linux) may offer free software "patches" to close holes in the system that hackers or phishers could exploit.

- **Be cautious about opening any attachment or downloading any files from emails you receive**, regardless of who sent them.
- **Report suspicious activity to the FTC.** If you get spam that is phishing for information, forward it to spam@uce.gov. If you believe you've been scammed, file your complaint at www.ftc.gov, and then visit the FTC's Identity Theft Web site at www.consumer.gov/idtheft to learn how to minimize your risk of damage from ID theft. Visit www.ftc.gov/spam to learn other ways to avoid email scams and deal with deceptive spam.

The FTC works for the consumer to prevent fraudulent, deceptive, and unfair business practices in the marketplace and to provide information to help consumers spot, stop, and avoid them. To file a complaint or to get free information on consumer issues, visit www.ftc.gov or call toll-free, 1-877-FTC-HELP (1-877-382-4357); TTY: 1-866-653-4261. The FTC enters Internet, telemarketing, identity theft, and other fraud-related complaints into Consumer Sentinel, a secure, online database available to hundreds of civil and criminal law enforcement agencies in the U.S. and abroad.

FRANK H. MURKOWSKI,
GOVERNOR

DEPARTMENT OF LAW

OFFICE OF THE ATTORNEY GENERAL

1031 WEST 4TH AVENUE, SUITE 200
ANCHORAGE, ALASKA 99501-5903
PHONE: (907)269-5100
FAX: (907)276-8554

Identity Theft Quiz
When Fact Becomes Fiction

For each correct answer, give yourself 10 points. For each incorrect answer, give yourself zero points. The grading scale is provided at the end of the quiz. Good luck.

1) True or False: ID theft is currently the fastest growing white collar crime in the U.S.

Answer: True: A survey commissioned by the Federal Trade Commission revealed that an estimated 27 million Americans have been victims of the crime in the last five years, nearly 10 million in the last year alone.

2) Identity thieves can get your personal information by:

a. Stealing your wallet or purse
b. Stealing your mail or completing a 'change of address form' without your knowledge
c. Rummaging through your trash at home or at a business, a practice known as "dumpster diving"
d. Using personal information they find on the Internet about you
e. All of the above

Answer: e: all of the above. And that's not all. For more ways thieves can steal your identity, visit www.consumer.gov/idtheft/understanding_idt.html#2.

3) True or False: When disposing of a computer, it's sufficient to delete files by using the keyboard or mouse commands.

Answer: False. The files may stay on your computer's hard drive. It's best to use a "wipe" utility program to overwrite the entire hard drive; it makes the files unrecoverable.

4) Once identity thieves get your personal information, they can use it to:

a. Call your credit card issuer and change the mailing address on the card
b. Open a new credit card account or bank account in your name
c. File for bankruptcy under your name to avoid paying off debts they've incurred
d. Counterfeit checks or drain your bank account
e. All of the above

Answer: e: all of the above. Identity thieves can use your personal information in a variety of ways to commit fraud.

5) To help minimize your risk of becoming a victim of ID theft, you should:

a. Not give out your personal information by email, Internet, phone or mail unless you initiated the contact and/or you are certain that you know who you're dealing with
b. Not carry your Social Security card with you
c. Carry only the identification information and the number of credit and debit cards that you'll actually need
d. Place passwords on your credit card, bank and phone accounts
e. All of the above.

Answer: e: all of the above. For more tips, visit www.consumer.gov/idtheft/protect_againstidt.html#5

6) True or False: If you are a victim of identity theft, it's a good idea to place a fraud alert on your credit reports and review your credit reports periodically. True or False.

Answer: True. The fraud alert on your credit report can help prevent an identity thief from opening additional accounts in your name.

7) If you think someone has stolen your personal information or identification, what should you do to prevent the misuse of that information:

a. Immediately close all your credit card or bank accounts
b. Place a fraud alert with any one of the three national consumer reporting companies
c. Contact the Social Security Administration to get a new Social Security number
d. Alert issuing agencies for your driver's license and other identification documents
e. All of the above

Answer: e: all of the above.

8) True or False: If you have a high speed connection to the Internet, such as DSL or a cable modem, you need a firewall program to help stop uninvited guests from accessing your computers.

Answer: True. A high-speed connection leaves your computer connected to the Internet 24 hours a day. If you don't have a firewall program, hackers can take over your computer and access personal information stored on it or use it to commit other crimes

9) You think you've been a victim of identity theft when you:

a. Fail to receive bills or other mail
b. Receive credit cards for which you didn't apply
c. Are denied credit for no apparent reason
d. Get calls or letters from debt collectors or businesses about merchandise or services you didn't buy
e. All of the above.

Answer: e: all of the above.

10) True or False: It's okay to keep your computer and website passwords on a piece of paper taped to your computer.

Answer: False. You should take care to safeguard your passwords. Also, it's a good idea to use a strong password - a combination of letters (upper and lower case), numbers and symbols.

Grading Scale

0 – 49: Study up. You could be putting yourself at increased risk for identity theft. Take care to secure your personal information and not give it out unless you know who you're dealing with; don't carry your Social Security card with you; guard your mail and trash from theft by depositing mail in a secure mailbox and shredding or tearing financial receipts or statements; and carefully review your bank and credit card statements.

50 -79: You could be more vigilant about the security of your personal information. You can lessen your risk by taking some of the above precautions, if you haven't already.

80 -100: Congratulations, you are taking precautions to avoid becoming a victim of ID theft. Keep it up and share your knowledge to make sure that friends, family and colleagues are doing the same.